AMENDMENTS TO THE CLAIMS

Please replace all previous versions of the claims with the following listing:

1. (Currently Amended) A machine ~~Machine~~ tool [[(2, 2a)]] protected against improper activation, comprising:

an open-loop or [[and/or]] closed-loop control device for the activation of machine functions~~, preferably machine axes (σ_1, σ_2)~~;

[[means]]a reading module for reading in machine control parameters for the open-loop or ~~and/or~~ closed-loop control device from a data carrier or electronic carrier signal [[(3),]]; and

an improper-activation safety module~~, preferably an improper-activation safety software module,~~ which decodes the machine control parameters [[again]] that are intended for the machine tool and are encoded ~~by means of~~ using an asymmetric encryption method, using an encryption key which is assigned to the machine tool [[(2, 2a)]] and provided for the encryption, with the aid of a decryption key which is likewise assigned to the machine tool [[(2, 2a)]], is different from the encryption key and is provided for the decryption, and which module enables the machine control parameters for controlling the machine tool [[(2, 2a)]] only in the case of successful decryption;

wherein the improper-activation safety module determines the successful decryption of the machine control parameters after decryption also on the basis of finding a signature of a unit authorized for activating the machine tool.

2. (Currently Amended) The machine ~~Machine~~ tool [[(2, 2a)]] protected against improper activation according to Claim 1, ~~characterized in that~~ wherein the machine tool has [[a]]the reading module~~, preferably a chip card reader,~~ which is intended for receiving a decryption module~~, preferably a chip card,~~ which has the decryption key, with the aid of which the improper-activation safety module

decodes the encoded machine control parameters, and the decryption module is set up in such a way that only the improper-activation safety module can read out the decryption key from the module.

3. (Cancelled)

4. (Currently Amended) The machine ~~Machine~~ tool [[(2, 2a)]] protected against improper activation according to Claim 1, ~~characterized in that~~ wherein the improper-activation safety module enables various functions of the machine tool [[(2, 2a)]] for control by the machine control parameters in dependence on the decryption key originating from a plurality of decryption keys assigned to the machine tool [[(2, 2a)]].

5. (Cancelled)

6. (Cancelled)

7. (Currently Amended) A method ~~Method~~ of avoiding improper machine activation by machine control parameters of a machine tool [[(2, 2a)]], comprising:

~~characterized in that the machine control parameters intended for the machine tool are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode the machine control parameters again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption~~

assigning a private encryption key and a private decryption key to a sender of the machine control parameters using a computer system, wherein the private encryption key is different from the private decryption key and is provided for the decoding;

first encoding the machine control parameters intended for the machine tool using the computer system and the private decryption key;

providing the first encoded machine control parameters with a sender identification of a sender using the computer system;

second encoding the provided machine control parameters using the computer system and an encryption key that is assigned to the machine tool;

first decoding the second encoded machine control parameters using the computer system and a decryption key that is assigned to the machine tool, wherein the decryption key is different from the encryption key and is provided for the decoding;

authenticating a sender by the sender's identification and a suitability of the private encryption key assigned to the sender for the first decoded machine control parameters using the computer system; and, if so,

second decoding the first decoded machine control parameters using the computer system and the private encryption key.

8. (Cancelled)

9. (Cancelled)

10. (Currently Amended) A computer ~~Computer~~ system ~~(1) with~~ comprising at least one data processing unit and at least one memory, ~~characterized in that~~ wherein the data processing unit is set up in programming terms in such a way that it works on the basis of the method according to Claim 7.

11. (Currently Amended) A computer readable medium ~~Computer program which has~~ comprising instructions ~~which are set up~~ for carrying out the method according to Claim 7.

12. (Cancelled)

13. (Cancelled)

14. (Currently Amended) A computer readable medium ~~Data carrier or electronic carrier signal (3) with machine control parameters~~ for reading

instructions into a machine tool [[(2, 2a)]], the machine tool being protected against improper activation, and having an open-loop or ~~and/or~~ closed-loop control device for the activation of machine functions~~, preferably machine axes (σ_1, σ_2);~~ [[means]] a reading module for reading in the instructions for the machine tool from the computer readable medium and machine control parameters for the open-loop or ~~and/or~~ closed-loop control device from a data carrier or electronic carrier signal [[(3);]], and an improper-activation safety module, ~~preferably an improper-activation safety software module,~~ which decodes the machine control parameters [[again]] that are intended for the machine tool using an encryption key and a private decryption key assigned to the machine tool, wherein the encryption key and the private decryption key are stored in the instructions~~, characterized in that;~~

~~on the data carrier or the electronic carrier signal there are machine control parameters for the machine tool (2, 2a) which are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode them again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption, and~~

wherein the machine control parameters for the machine tool are first encoded using a private encryption key assigned to a sender of the machine control parameters, and are provided with a sender identification of the sender, and, signed in this way, are only encoded using the encryption key that is assigned to the machine tool and known for the encryption;

so that, when the machine tool decodes the machine control parameters using the private decryption key, the machine tool authenticates a sender by the sender's identification and a suitability of an encryption key assigned to the sender's identification for the decryption of the machine control parameters intended for the machine tool; and

wherein the data carrier or the electronic carrier signal [[(3)]] controls the machine tool ~~(2, 2a) by means of~~ using [[these]]the machine control parameters during reading-in or after reading-in after [[they]]the machine control parameters have been decoded.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (New) A method of avoiding improper machine activation by machine control parameters of a machine tool according to Claim 7, further comprising:

checking whether the machine control parameters were actually generated for said machine tool using the computer system.

27. (New) A method of avoiding improper machine activation by machine control parameters of a machine tool according to Claim 26, further comprising:

determining whether a module associated with a sender which generated the machine control parameters is actually suitable and authorized to do so using the computer system.